(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

Event 22

Date/Time: (when tests conducted)

March 20, 1997 0925

Location: (where tests orchestrated from)

Fleet Information Warfare Center, NAB Little Creek
Norfolk, VA

Participants: (who was present during tests)
Arnold Llamas, FIWC/QVESTECH
Norm Beebe, NSGA Pensacola
Stacy Smathers, NSGA Pensacola
Lt. Nina Kenmore, FIWC

Hardware Complement: (model/designations of major equipment used during tests)
Sun Ultra 1 Creator - Director
Borderguard 2000 - Router
NetRanger NSX - Sensor
Gateway 2000 - Target
W/Red Hat LINUX

Major Events: (plain English dialog of events)

Run attack signatures 4 or 5 times to all sensors.

Result Summary: (observer conclusions)

Satisfactorily verified

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

Event 23

Date/Time: (when tests conducted)

March 20, 1997 0925

Location: (where tests orchestrated from)

Fleet Information Warfare Center, NAB Little Creek
Norfolk, VA

Participants: (who was present during tests)
Arnold Llamas, FIWC/QVESTECH
Norm Beebe, NSGA Pensacola
Stacy Smathers, NSGA Pensacola
Lt. Nina Kenmore, FIWC

Hardware Complement: (model/designations of major equipment used during tests)
Sun Ultra 1 Creator - Director
Borderguard 2000 - Router
NetRanger NSX - Sensor
Gateway 2000 - Target
W/Red Hat LINUX

Major Events: (plain English dialog of events)

Operators see that multiple attacks have been automatically consolidated into a single icon.

Result Summary: (observer conclusions)

Satisfactorily verified

Multiple attacks consolidated on yellow icons

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

Event 24

Date/Time: (when tests conducted)

March 20, 1997 1004

Location: (where tests orchestrated from)

Fleet Information Warfare Center, NAB Little Creek
Norfolk, VA

Participants: (who was present during tests)

Arnold Llamas, FIWC/QVESTECH
Norm Beebe, NSGA Pensacola
Stacy Smathers, NSGA Pensacola
Lt. Nina Kenmore, FIWC

Hardware Complement: (model designations of major equipment used during tests)
Sun Ultra 1 Creator - Director
Borderguard 2000 - Router
NetRanger NSX - Sensor
Gateway 2000 - Target
W/Red Hat LINUX

Major Events: (plain English dialog of events)

Run level 2 attack signature

Result Summary: (observer conclusions)

Satisfactorily verified

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

Event 25

Date/Time: (when tests conducted)

March 20, 1997 1004

Location: (where tests orchestrated from)

Fleet Information Warfare Center, NAB Little Creek
Norfolk, VA

Participants: (who was present during tests)

Arnold Llamas, FIWC/QVESTECH
Norm Beebe, NSGA Pensacola
Lt. Nina Kenmore, FIWC

Hardware Complement: (model/designations of major equipment used during tests)
Sun ultra 1 Creator - Director
Borderguard 2000 - Router
NetRanger NSX - Sensor
Gateway 2000 - Target
W/Red Hat LINUX

Major Events: (plain English dialog of events)

Run level 5 attack signature and view propagation of director display hierarchy

Result Summary: (observer conclusions)

Satisfactorily verified

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

Event 26

Date/Time: (when tests conducted)

March 18, 1997 1630

Location: (where tests orchestrated from)

Fleet Information Warfare Center, NAB Little Creek
Norfolk, VA

Participants: (who was present during tests)

Arnold Llamas, FIWC/QVESTECH
Norm Beebe, NSGA Pensacola
Stacy Smathers, NSGA Pensacola
Lt. Nina Kenmore, FIWC

Hardware Complement: (model/designations of major equipment used during tests)
Sun Ultra 1 Creator - Director
BorderGuard 2000 - Router
NetRanger - NSX - Sensor
Gateway 2000 - Target
W/ Red Hat LINUX

Major Events: (plain English dialog of events)

Configure Director to generate automatic Email and/or pages

Result Summary: (observer conclusions)

Satisfactorily verified

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

Event 27

Date/Time: (when tests conducted)

March 18, 1997 1630

Location: (where tests orchestrated from)

Fleet Information Warfare Center, NAB Little Creek
Norfolk, VA

Participants: (who was present during tests)

Arnold Llamas, FIWC/QVESTECH
Norm Beebe, NSGA Pensacola
Stacy Smathers, NSGA Pensacola
Lt. Nina Kenmore, FIWC

Hardware Complement: (model designations of major equipment used during tests)
Sun Ultra 1 Creator - Director
Borderguard 2000 - Router
NetRanger NSX - Sensor
Gateway 2000 - Target
W/Red Hat LINUX

Major Events: (plain English dialog of events)

Run attack and observe E-mail and or pager activation

Result Summary: (observer conclusions)

Satisfactorily verified

FIWC VAAP tools were run on our office LAN
Level 5 Alarms were received by Email /pager

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

Event 28

Date/Time: (when tests conducted)

March 20, 1997 1243

Location: (where tests orchestrated from)
Fleet Information Warfare Center, NAB Little Creek
Norfolk, VA

Participants: (who was present during tests)
Arnold Llamas, FIWC/QVESTECH
Norm Beebe, NSGA Pensacola
Stacy Smathers, NSGA Pensacola
Lt. Nina Kenmore, FIWC

Hardware Complement: (model/designations of major equipment used during tests)
Sun Ultra 1 Creator - Director
Borderguard 2000 - Router
NetRanger NSX - Sensor
Gateway 2000 - Target
W/Red Hat LINUX

Major Events: (plain English dialog of events)

Attempt RLOGIN connect to a protected host from a machine authorized access to the network and observe alarm generated

Result Summary: (observer conclusions)

Satisfactorily verified

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

Event 31

Date/Time: (when tests conducted)

March 20, 1997 1614

Location: (where tests orchestrated from)

Fleet Information Warfare Center, NAB Little Creek
Norfolk, VA

Participants: (who was present during tests)
Arnold Llamas, FIWC/QVESTECH
Norm Beebe, NSGA Pensacola
Stacy Smathers, NSGA Pensacola
Lt. Nina Kenmore, FIWC

Hardware Complement: (model/designations of major equipment used during tests)
Sun Ultra 1 Creator - Director
Borderguard 2000 - Router
NetRanger NSX - Sensor
Gateway 2000 - Target
W/Red Hat LINUX

Major Events: (plain English dialog of events)

Telnet into target host and generate atomic alarm

Result Summary: (observer conclusions)

Satisfactory alarm

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

Event 32

Date/Time: (when tests conducted)

March 20, 1997

Location: (where tests orchestrated from)

Fleet Information Warfare Center, NAB Little Creek
Norfolk, VA

Participants: (who was present during tests)

Arnold Llamas, FIWC/QVESTECH
Norm Beebe, NSGA Pensacola
Stacy Smathers, NSGA Pensacola
Lt. Nina Kenmore, FIWC

Hardware Complement: (model/designations of major equipment used during tests)
Sun Ultra 1 Creator - Director
Borderguard 2000 - Router
NetRanger NSX - Sensor
Gateway 2000 - Target
W/ Red Hat LINUX

Major Events: (plain English dialog of events)

Run Port Sweep against host and observe composite alarm

Result Summary: (observer conclusions)

Satisfactorily verified.

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

Event 33

Date/Time: (when tests conducted)

March 20 1997, 1716

Location: (where tests orchestrated from)

Fleet Information Warfare Center - NAB Little Creek
Norfolk, VA

Participants: (who was present during tests)

Arnold Llamas, FIWC/QVESTECH
Norm Beebe, NSGA Pensacola
Stacy Smathers, NSGA Pensacola
Lt. Nina Ksenmore, FIWC

Hardware Complement: (model/designations of major equipment used during tests)
Sun Ultra 1 Creator - Director
Borderguard 2000 - Router
NetRanger NSX - Sensor
Gateway 2000 - Target
W/Red Hat LINUX

Major Events: (plain English dialog of events)

Run SATAN in heavy mode and observe corresponding composite alarm.

Result Summary: (observer conclusions)

Satisfactorily verified

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

Event 34

Date/Time: (when tests conducted)

March 20, 1997

Location: (where tests orchestrated from)

Fleet Information Warfare Center, NAB Little Creek
Norfolk, VA

Participants: (who was present during tests)

Arnold Llamas, FIWC/QVESTECH
Norm Beebe, NSGA Pensacola
Stacy Smathers, NSGA {Pensacola
Lt. Nina Kenmore, FIWC

Hardware Complement: (model/designations of major equipment used during tests)
Sun Ultra 1 Creator - Director
Borderguard 2000 - Router
NetRanger NSX - Sensor
Gateway 2000 - Target
w/Red Hat LINUX

Major Events: (plain English dialog of events)

Run SATAN in light mode and observe corresponding composite alarm

Result Summary: (observer conclusions)

Satisfactory, alarm

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

Event 35

Date/Time: (when tests conducted)

March 20, 1997

Location: (where tests orchestrated from)

Fleet Information Warfare Center, NAB Little Creek
Norfolk, VA

Participants: (who was present during tests)

Arnold Llamas, FIWC/QVESTECH
Norm Beebe, NSGA Pensacola
Stacy Smathers, NSGA Pensacola
Lt. Nina Kenmore, FIWC

Hardware Complement: (model/designations of major equipment used during tests)
Sun Ultra 1 Creator - Director
Borderguard 2000 - Router
NetRanger NSX - Sensor
Gateway 2000 - Target
W/Red Hat LINUX

Major Events: (plain English dialog of events)

Set NSX to Autoshun Telnet attempt. Attempt telnet and observe Autoshun occurs.

Result Summary: (observer conclusions)

Satisfactorily verified

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

Event 36

Date/Time: (when tests conducted)

March 20, 1997

Location: (where tests orchestrated from)

Fleet Information Warfare Center, NAB Little Creek
Norfolk, VA

Participants: (who was present during tests)

Arnold Llamas, FIWC/QVESTECH
Norm Beebe, NSGA Pensacola
Stacy Smathers, NSGA Pensacola
Lt. Nina Kenmore, FIWC

Hardware Complement: (model/designations of major equipment used during tests)
Sun Ultra 1 Creator - Director
Borderguard 2000 - Router
NetRanger NSX - Sensor
Gateway 2000 - Target
W/Red Hat LINUX

Major Events: (plain English dialog of events)

Attempt Telnet and Operator manually responds w/ Shun

Result Summary: (observer conclusions)

Satisfactorily verified

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

Event 38

Date/Time: (when tests conducted)

March 21, 1997

Location: (where tests orchestrated from)

Fleet Information Warfare Center, NAB Little Creek
Norfolk, VA

Participants: (who was present during tests)

Arnold Llamas, FIWC/QVESTECH
Norm Beebe, NSGA Pensacola
Stacy Smathers, NSGA Pensacola
Lt. Nina Kenmore, FIWC

Hardware Complement: (model/designations of major equipment used during tests)
Sun Ultra 1 Creator - Director
Borderguard 2000 - Router
NetRanger NSX - Sensor
Gateway 2000 - Target
W/Red Hat LINUX

Major Events: (plain English dialog of events)

Configure NSX to log keystrokes from specified attack type

Result Summary: (observer conclusions)

Satisfactorily verified
Attack type = Telnet w/'IFS=/'

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

Event 39

Date/Time: (when tests conducted)

March 21, 1997

Location: (where tests orchestrated from)

Fleet Information Warfare Center, NAB Little Creek
Norfolk, VA

Participants: (who was present during tests)

Arnold Llamas, FIWC/QVESTECH
Norm Beebe, NSGA Pensacola
Stacy Smathers, NSGA Pensacola
Lt. Nina Kenmore, FIWC

Hardware Complement: (model/designations of major equipment used during tests)
Sun Ultra 1 Creator - Director
Borderguard 2000 - Router
NetRanger NSX - Sensor
Gateway 2000 - Target
W/ Red Hat LINUX

Major Events: (plain English dialog of events)

Run attack and verify that keystroke capture occurs

Result Summary: (observer conclusions)

Satisfactorily verified
Keystroke logs show one NSX, However, the 'transcript command was difficult to use compared to nid's "iscript" command. No command-line arguments are required for 'iscript' other the filename
Too many steps to see data
Very cumbersome

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

Event 40

Date/Time: (when tests conducted)

March 24, 1997

Location: (where tests orchestrated from)

Fleet Information Warfare Center, NAB Little Creek
Norfolk, VA

Participants: (who was present during tests)

Arnold Llamas, FIWC/QVESTECH
Norm Beebe, NSGA Pensacola
Stacy Smathers, NSGA Pensacola
Lt. Nina Kenmore, FIWC

Hardware Complement: (model/designations of major equipment used during tests)
Sun Ultra 1 Creator - Director
Borderguard 2000 - Router
NetRanger NSX - Sensor
Gateway 2000 - Target
W/Red Hat LINUX

Major Events: (plain English dialog of events)

Configure NSX to dump Event and IP Session logs to an archive device.

Result Summary: (observer conclusions)

Satisfactorily verified

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

Event 41

Date/Time: (when tests conducted)

March 24, 1997

Location: (where tests orchestrated from)

Fleet Information Warfare Center, NAB Little Creek
Norfolk, VA

Participants: (who was present during tests)

Arnold Llamas, FIWC/QVESTECH
norm Beebe, NSGA Pensacola
Stacy Smathers, NSGA Pensacola
Lt. Nina Kenmore, FIWC

Hardware Complement: (model/designations of major equipment used during tests)
Sun Ultra 1 Creator - Director
Borderguard 2000 - Router
NetRanger NSX - Sensor
Gateway 2000 - Target
W/Red Hat LINUX

Major Events: (plain English dialog of events)

Verify that data has transferred to off-line device.

Result Summary: (observer conclusions)

Satisfactorily verified by checking contents of tape.

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

Event 42

Date/Time: (when tests conducted)

March 18, 1997

Location: (where tests orchestrated from)

Fleet Information Warfare Center, NAB Little Creek
Norfolk, VA

Participants: (who was present during tests)

Arnold Llamas, FIWC/QVESTECH
Norm Beebe, NSGA Pensacola
Stacy Smathers, NSGA Pensacola
Lt. Nina Kenmore, FIWC

Hardware Complement: (model/designations of major equipment used during tests)
Sun Ultra 1 Creator - Director
Borderguard 2000 - Router
NetRanger NSX - Sensor
Gateway 2000 - Target
W/Red Hat LINUX

Major Events: (plain English dialog of events)

Run attack to generate alarm

Highlight alarm and note information displayed

Result Summary: (observer conclusions)

satisfactorily verified

In house VAAO was run to generate level 5 alarm

LIWA REPORTS

(MASTER)

Interrogation Forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER:

SCRIPT REFERENCE: none

Date/Time: begin 19-Mar-97, 9:00am; end 20-Mar-97

Location: LIWA

Participants: Michelle Pagan, LIWA /TASC; Tim Collins, BTG

Hardware Compliment: Borderguard SR04, Director: SUN Ultra-1, NSX 2000

Software Complement: NetRanger Director v1.2.2, SunOS 5.5.1, SunOS nsx 5.5 i86pc I386

Major Events:

Result Summary:

REFERENCE EVENT NUMBER: 7

Major Events: Observed TCP Port Sweep level 5 alarm

Result Summary: Successfully verified.

REFERENCE EVENT NUMBER: 8

Major Events: Changed from level 5 to level 4 alarm; performed nrget of SigOfGeneral

Result Summary: Successfully verified.

REFERENCE EVENT NUMBER: 11

Major Events: Verified all privileges available via nr.postofficed/RecordOfAuths

Result Summary: Successfully verified.

REFERENCE EVENT NUMBER: 12

Major Events: Removed NRGETBULK from privileges via nrset; verified NRGETBULK not available --> insufficient privileges

Result Summary: Successfully verified.

REFERENCE EVENT NUMBER: 19

Major Events: Observed TCP Port Sweep alarm from 208.213.191.4; shunned IP source; verified shun via nrmanaged/ShunHostList/nrget; unshunned source via nrmanaged/unShunAll/nrexec; verified no shunned hosts via nrmanaged/ShunHostList/nrget = error

Result Summary: Successfully verified.

Note: When using Security/Unshun/IP Source, the result is /usr/bin/sh: /usr/nr/bin/nrUnshunHost: not found. Checked for file, verified file doesn't exist.

REFERENCE EVENT NUMBER: 22/23

Major Events: Observed three TCP Port Sweeps and numerous INCOM1_TCP_FAIL,4

Result Summary: Successfully verified.

REFERENCE EVENT NUMBER: 24

Major Events: Observed INCOM1_TCP_FAIL level 3 alarms at LIWA but not at AFIWC or BCBL

Result Summary: Successfully verified.

REFERENCE EVENT NUMBER: 25

Major Events: Observed TCP PORT SWEEP level 4 alarms at LIWA and AFIWC, not BCBL

Result Summary: Successfully verified.

Note: BCBL was not included in this test. TCP PORT SWEEP was changed from level 5 to level 4 in event 8

REFERENCE EVENT NUMBER: 28

Major Events: Observed INCOM1_LOGIN_FAIL,2 alarms

Result Summary: Successfully verified

REFERENCE EVENT NUMBER 29

Major Events: Observed MAIL recon level 3 alarm

Result Summary: Successfully verified

Note: When using Show Current Events, was not able to view current events during any test.

REFERENCE EVENT NUMBER 30

Major Events: Configure new string signature via nr.sensord/RecordofString/nrset to 4001 25 3 1 "foo bar" and nr.sensord/SigofString/nrset to 4001 0 4 4 4 4 0...;; Received Match: foo bar level 4 alarm.

Result Summary: Successfully verified

REFERENCE EVENT NUMBER 31

Major Events: Observed IFS=/ level 5 alarm at LIWA, AFIWC, and BCBL.

Result Summary: Successfully verified

Note: This is the first time receiving alarms from BCBL.

REFERENCE EVENT NUMBER: 32

Major Events: Observed fifteen INCOM1_TCP_FAIL,4 level 3 alarms and one TCP_PORT_SWEEP level 4 composite alarm.

Result Summary: Successfully verified.

REFERENCE EVENT NUMBER: 33/34

Major Events: Ran E-SATAN (developed by MITRE) in heavy and light mode from internal host to target (128.190.161.18). Triggered numerous alarms but not a SATAN alarm.

Result Summary: Unsuccessful.

Note: COACT's SATAN is the only legal scanning source for SPOCK and was unavailable. ACERT performed a SATAN scan from an internal host using E-SATAN. In light mode, E-SATAN performed dns and udpscan. NetRanger produced INCOM1_UDP_FAIL,11 alarms. In heavy mode, E-SATAN performed dns, tcpscan, portscan, and udpscan. NetRanger produced INCOM1_TCP_FAIL, INCOM1_GOPHER_FAIL, and INCOM1_UDP_FAIL alarms. In either mode, NetRanger did not report a SATAN alarm. FIWC was successful with this test.

REFERENCE EVENT NUMBER: 35

Major Events: Configure signature 301 (IFS=/) to autoshun via nrsensord/SigOfStringMatch/nrset to 301 1 5 5 5 5 0...; Observed Match: IFS=/ level 5 alarm; Verified autoshun hosts via nr.managed/ShunHostList/nrget.

Result Summary: Successfully verified.

Note: ShunHostList included both the source (208.213.191.4) and the target (128.190.161.18). NetRanger has the capability to specify in which direction an alarm is triggered. The 301 signature could have been configured to alarm on the client portion of the telnet session, thereby shunning the source only. Careful consideration should be exercised when using this feature.

REFERENCE EVENT NUMBER: 36

Major Events:

Result Summary: Successfully verified in event 19.

REFERENCE EVENT NUMBER: 38

Major Events: Configure signature 301 (IFS=/) via nrsensord/SigOfString/nrset to 301 2 5 5 5 5 0... to log keystrokes; verified via nrsensord/SigOfString/nrgetbulk

Result Summary: Successfully verified.

REFERENCE EVENT NUMBER: 39

Major Events: Observed Match: IFS=/ alarm.

Result Summary: Partially successful. Unable to verify keystrokes in log file /usr/nr/var/iplog/iplog.128.190.161.18 (target) or iplog.208.213.191.4.

Note: The objective was to verify that the keystroke capture occurs. However, the iplog produced is a binary file and unreadable without the use of *transcript*. We were unable to verify the contents of the iplog. Suggest including a menu option that allows easy reading of the keystroke capture logs.

REFERENCE EVENT NUMBER: 42

Major Events:

Result Summary: Successfully verified via other events that generated alarms.

REFERENCE EVENT NUMBER: 43

Major Events:

Result Summary: Successfully verified via other events that generated alarms.

NSA REPORTS

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

10

Script Reference: (data files used during exercises for input/penetration/exercising, etc. Supply references on disk if possible for inclusion in final report, AND HARDCOPY FOR SURE.)

Intentionally Misconfigure and Show Error Logged.

Date/Time:(when tests conducted)

03/19/97 - 1349 hrs.

Location:(where tests orchestrated from)

National Security Agency (NSA)
DECIN Laboratory
FANX3
Room B4120

Participants:(who was present during tests)

Charles Freeman, V21

James Codespote, Y44

Linda Jessen, R23

Hardware Complement: (model/designations of major equipment used during tests)

Director - Sun SPARC 20
Target - Sun SPARC 5
Sensor - NSX
Routers (2) - NSC Border Guard 2000

Software Complement: (generic names of major software used during tests)

Director - Solaris 2.5
HP Openview - 4.11

Test Equipment: (Model/designations of major test equipment used during testing)

Protocol Analyzer - Wandel & Goltermann DA-30

Result Summary: (observer conclusions)

managed.conf - manually changed passwd for network device.

Did not change using GUI.

Claims: Manually Verified

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

11 & 12

Script Reference: (data files used during exercises for input/penetration/exercising, etc. Supply references on disk if possible for inclusion in final report, AND HARDCOPY FOR SURE.)

Confirm Specific Action is Allowed

Remove Previous Action from Director's Authorization and show Failure to Execute Specific Action.

Date/Time:(when tests conducted)

03/19/97 - 1405 hrs.

Location:(where tests orchestrated from)

National Security Agency (NSA)
DECIN Laboratory
FANX3
Room B4120

Participants:(who was present during tests)

Charles Freeman, V21

James Codespote, Y44

Linda Jessen, R23

Hardware Complement: (model/designations of major equipment used during tests)

Director - Sun SPARC 20
Target - Sun SPARC 5
Sensor - NSX
Routers (2) - NSC Border Guard 2000

Software Complement: (generic names of major software used during tests)

Director - Solaris 2.5
HP Openview - 4.11

Test Equipment: (Model/designations of major test equipment used during testing)

Protocol Analyzer - Wandel & Goltermann DA-30

Result Summary: (observer conclusions)

Claims: Verified

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

17 & 18

Script Reference: (data files used during exercises for input/penetration/exercising, etc. Supply references on disk if possible for inclusion in final report, AND HARDCOPY FOR SURE.)

Perform *getbulk* Command to Multiple NSXs from Single Director.

Alter Configuration of Multiple NSXs from Single Director.

Date/Time:(when tests conducted)

03/19/97 - 1421 hrs.

Location:(where tests orchestrated from)

National Security Agency (NSA)
DECIN Laboratory
FANX3
Room B4120

Participants:(who was present during tests)

Charles Freeman, V21

James Codespote, Y44

Linda Jessen, R23

Hardware Complement: (model/designations of major equipment used during tests)

Director - Sun SPARC 20
Target - Sun SPARC 5
Sensor - NSX
Routers (2) - NSC Border Guard 2000

Software Complement: (generic names of major software used during tests)

Director - Solaris 2.5
HP Openview - 4.11

Test Equipment: (Model/designations of major test equipment used during testing)

Protocol Analyzer - Wandel & Goltermann DA-30

Result Summary: (observer conclusions)

Claims: Verified

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

19

Script Reference: (data files used during exercises for input/penetration/exercising, etc. Supply references on disk if possible for inclusion in final report, AND HARDCOPY FOR SURE.)

Operator Applies *SHUN* to ongoing attack.

Date/Time:(when tests conducted)

03/19/97 - 1444 hrs.

Location:(where tests orchestrated from)

National Security Agency (NSA)
DECIN Laboratory
FANX3
Room B4120

Participants:(who was present during tests)

Charles Freeman, V21

James Codespote, Y44

Linda Jessen, R23

Hardware Complement: (model/designations of major equipment used during tests)

Director - Sun SPARC 20
Target - Sun SPARC 5
Sensor - NSX
Routers (2) - NSC Border Guard 2000

Software Complement: (generic names of major software used during tests)

Director - Solaris 2.5
HP Openview - 4.11

Test Equipment: (Model/designations of major test equipment used during testing)

Protocol Analyzer - Wandel & Goltermann DA-30

Result Summary: (observer conclusions)

Claims: Verified.

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

20 & 21

Script Reference: (data files used during exercises for input/penetration/exercising, etc. Supply references on disk if possible for inclusion in final report, AND HARDCOPY FOR SURE.)

Attack 3 NSXs to produce Red, Yellow and Green Icons.

Reset Threshold to Produce all Yellow Icons When Same set of Attacks ran a Second Time.

Date/Time:(when tests conducted)

03/19/97 - 1508 - 1640 hrs.

03/20/97 - 0905 hrs.

Location:(where tests orchestrated from)

National Security Agency (NSA)
DECIN Laboratory
FANX3
Room B4120

Participants:(who was present during tests)

Charles Freeman, V21

James Codespote, Y44

Linda Jessen, R23

Hardware Complement: (model/designations of major equipment used during tests)

Director - Sun SPARC 20
Target - Sun SPARC 5
Sensor - NSX
Routers (2) - NSC Border Guard 2000

Software Complement: (generic names of major software used during tests)

Director - Solaris 2.5
HP Openview - 4.11

Test Equipment: (Model/designations of major test equipment used during testing)

Protocol Analyzer - Wandel & Goltermann DA-30

Result Summary: (observer conclusions)

03/19/97 & 03/20/97

NSA target machine had configuration problems during this test. Test scenario verified by FIWC per Spock.

System problems rectified after this test was completed.

Claims: Verified at FIWC

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

22 & 23

Script Reference: (data files used during exercises for input/penetration/exercising, etc. Supply references on disk if possible for inclusion in final report, AND HARDCOPY FOR SURE.)

Run attack signature 4 or 5 times to all sensors.

Operators see that multiple attacks have been automatically consolidated into a single icon.

Date/Time:(when tests conducted)

03/20/97 - 0916 hrs.

Location:(where tests orchestrated from)

National Security Agency (NSA)
DECIN Laboratory
FANX3
Room B4120

Participants:(who was present during tests)

Charles Freeman, V21

James Codespote, Y44

Linda Jessen, R23

Hardware Complement: (model/designations of major equipment used during tests)

Director - Sun SPARC 20
Target - Sun SPARC 5
Sensor - NSX
Routers (2) - NSC Border Guard 2000

Software Complement: (generic names of major software used during tests)

Director - Solaris 2.5
HP Openview - 4.11

Test Equipment: (Model/designations of major test equipment used during testing)

Protocol Analyzer - Wandel & Goltermann DA-30

Result Summary: (observer conclusions)

Our NetRanger Director got confused, had to kill openview and restart. All functions returned to normal.

Claims: Verified

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

24 & 25

Script Reference: (data files used during exercises for input/penetration/exercising, etc. Supply references on disk if possible for inclusion in final report, AND HARDCOPY FOR SURE.)

Run level two attack signature.

Run level 5 attack signature and view propagation of Director display hierarchy.

Date/Time:(when tests conducted)

03/20/97 - 1010 hrs.

Location:(where tests orchestrated from)

National Security Agency (NSA)
DECIN Laboratory
FANX3
Room B4120

Participants:(who was present during tests)

Charles Freeman, V21

James Codespote, Y44

Linda Jessen, R23

Hardware Complement: (model/designations of major equipment used during tests)

Director - Sun SPARC 20
Target - Sun SPARC 5
Sensor - NSX
Routers (2) - NSC Border Guard 2000

Software Complement: (generic names of major software used during tests)

Director - Solaris 2.5
HP Openview - 4.11

Test Equipment: (Model/designations of major test equipment used during testing)

Protocol Analyzer - Wandel & Goltermann DA-30

Result Summary: (observer conclusions)

Claims: Verified

NETRANGER EXERCISE

NATIONAL SECURITY AGENCY PARTICIPATION

PHASE II

19 - 21 MARCH 1997

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

28

Script Reference: (data files used during exercises for input/penetration/exercising, etc. Supply references on disk if possible for inclusion in final report, AND HARDCOPY FOR SURE.)

Attempt *rlogin* connect to protected host from a machine authorized access to the network and observe alarm generated.

Date/Time:(when tests conducted)

03/20/97 - 1237 hrs.

Alarm Level:

3

Location:(where tests orchestrated from)

National Security Agency (NSA)
DECIN Laboratory
FANX3
Room B4120

Participants:(who was present during tests)

Charles Freeman, V21

James Codespote, Y44

Linda Jessen, R23

Hardware Complement: (model/designations of major equipment used during tests)

Director - Sun SPARC 20
Target - Sun SPARC 5
Sensor - NSX
Routers (2) - NSC Border Guard 2000

Software Complement: (generic names of major software used during tests)

Director - Solaris 2.5
HP Openview - 4.11

Test Equipment: (Model/designations of major test equipment used during testing)

Protocol Analyzer - Wandel & Goltermann DA-30

Result Summary: (observer conclusions)

Incom_login_Fail, 3 icon appeared on Director - indicates 3 failed login attempts.

Claims: Verified

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

29

Script Reference: (data files used during exercises for input/penetration/exercising, etc. Supply references on disk if possible for inclusion in final report, AND HARDCOPY FOR SURE.)

Execute *sendmail* attack and observe alarm generation.

Date/Time:(when tests conducted)

03/20/97 - 1241 hrs.

Alarm Level:

3

Location:(where tests orchestrated from)

National Security Agency (NSA)
DECIN Laboratory
FANX3
Room B4120

Participants:(who was present during tests)

Charles Freeman, V21

James Codespote, Y44

Linda Jessen, R23

Hardware Complement: (model/designations of major equipment used during tests)

Director - Sun SPARC 20
Target - Sun SPARC 5
Sensor - NSX
Routers (2) - NSC Border Guard 2000

Software Complement: (generic names of major software used during tests)

Director - Solaris 2.5
HP Openview - 4.11

Test Equipment: (Model/designations of major test equipment used during testing)

Protocol Analyzer - Wandel & Goltermann DA-30

Result Summary: (observer conclusions)

Mail: Recon icon appeared - using network analyzer saw 8 packets came across before alarm tripped.

Claims: Verified

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

30

Script Reference: (data files used during exercises for input/penetration/exercising, etc. Supply references on disk if possible for inclusion in final report, AND HARDCOPY FOR SURE.)

Attempt to send email with content identified as a policy violation and observe alarm generation.

Date/Time:(when tests conducted)

03/20/97 - 1301 hrs.

Alarm Level:

5

Location:(where tests orchestrated from)

National Security Agency (NSA)
DECIN Laboratory
FANX3
Room B4120

Participants:(who was present during tests)

Charles Freeman, V21

James Codespote, Y44

Linda Jessen, R23

Hardware Complement: (model/designations of major equipment used during tests)

Director - Sun SPARC 20
Target - Sun SPARC 5
Sensor - NSX
Routers (2) - NSC Border Guard 2000

Software Complement: (generic names of major software used during tests)

Director - Solaris 2.5
HP Openview - 4.11

Test Equipment: (Model/designations of major test equipment used during testing)

Protocol Analyzer - Wandel & Goltermann DA-30

Result Summary: (observer conclusions)

2 Match IFS=/ icons appear - alarm source 208.213.191.4, alarm source 144.51.132.98 caught both ways, coming in and echo back.

Claims: Verified

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

32

Script Reference: (data files used during exercises for input/penetration/exercising, etc. Supply references on disk if possible for inclusion in final report, AND HARDCOPY FOR SURE.)

Run port sweep against host and observe composite alarm.

Date/Time:(when tests conducted)

03/20/97 - 1340 hrs.

Alarm Level:

5

Location:(where tests orchestrated from)

National Security Agency (NSA)
DECIN Laboratory
FANX3
Room B4120

Participants:(who was present during tests)

Charles Freeman, V21

James Codespote, Y44

Linda Jessen, R23

Hardware Complement: (model/designations of major equipment used during tests)

Director - Sun SPARC 20
Target - Sun SPARC 5
Sensor - NSX
Routers (2) - NSC Border Guard 2000

Software Complement: (generic names of major software used during tests)

Director - Solaris 2.5
HP Openview - 4.11

Test Equipment: (Model/designations of major test equipment used during testing)

Protocol Analyzer - Wandel & Goltermann DA-30

Result Summary: (observer conclusions)

TCP Port Sweep icon appeared.

Claims: Verified

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

31

Script Reference: (data files used during exercises for input/penetration/exercising, etc. Supply references on disk if possible for inclusion in final report, AND HARDCOPY FOR SURE.)

Telnet into target host and generate atomic alarm.

Date/Time:(when tests conducted)

03/20/97 - 1241 hrs.

Alarm Level:

3

Location:(where tests orchestrated from)

National Security Agency (NSA)
DECIN Laboratory
FANX3
Room B4120

Participants:(who was present during tests)

Charles Freeman, V21

James Codespote, Y44

Linda Jessen, R23

Hardware Complement: (model/designations of major equipment used during tests)

Director - Sun SPARC 20
Target - Sun SPARC 5
Sensor - NSX
Routers (2) - NSC Border Guard 2000

Software Complement: (generic names of major software used during tests)

Director - Solaris 2.5
HP Openview - 4.11

Test Equipment: (Model/designations of major test equipment used during testing)

Protocol Analyzer - Wandel & Goltermann DA-30

Result Summary: (observer conclusions)

Mail: Recon icon appeared - using network analyzer saw 8 packets come across before alarm tripped.

Claims: Verified

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

35

Script Reference: (data files used during exercises for input/penetration/exercising, etc. Supply references on disk if possible for inclusion in final report, AND HARDCOPY FOR SURE.)

Set NSX to autoshun telnet attempt. Attempt telnet and observe autoshun occur.

Date/Time:(when tests conducted)

03/20/97 - 1416 hrs.

Alarm Level:

5

Location:(where tests orchestrated from)

National Security Agency (NSA)
DECIN Laboratory
FANX3
Room B4120

Participants:(who was present during tests)

Charles Freeman, V21

James Codespote, Y44

Linda Jessen, R23

Hardware Complement: (model/designations of major equipment used during tests)

Director - Sun SPARC 20
Target - Sun SPARC 5
Sensor - NSX
Routers (2) - NSC Border Guard 2000

Software Complement: (generic names of major software used during tests)

Director - Solaris 2.5
HP Openview - 4.11

Test Equipment: (Model/designations of major test equipment used during testing)

Protocol Analyzer - Wandel & Goltermann DA-30

Result Summary: (observer conclusions)

Match: IFS=/ icons appeared - alarm source 208.213.191.4, alarm source 144.51.132.98 caught both ways, coming in and echo back.

Claims: Verified

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

36

Script Reference: (data files used during exercises for input/penetration/exercising, etc. Supply references on disk if possible for inclusion in final report, AND HARDCOPY FOR SURE.)

Attempt telnet and operator manually respond with shun.

Date/Time:(when tests conducted)

03/20/97 - 1507 hrs.

Alarm Level:

4

Location:(where tests orchestrated from)

National Security Agency (NSA)
DECIN Laboratory
FANX3
Room B4120

Participants:(who was present during tests)

Charles Freeman, V21

James Codespote, Y44

Linda Jessen, R23

Hardware Complement: (model/designations of major equipment used during tests)

Director - Sun SPARC 20
Target - Sun SPARC 5
Sensor - NSX
Routers (2) - NSC Border Guard 2000

Software Complement: (generic names of major software used during tests)

Director - Solaris 2.5
HP Openview - 4.11

Test Equipment: (Model/designations of major test equipment used during testing)

Protocol Analyzer - Wandel & Goltermann DA-30

Result Summary: (observer conclusions)

Match: /etc/shadow icon appeared - Alarm Name - String match

Netranger operator manually shunned address of attacker.

Claims: Verified

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

37

Script Reference: (data files used during exercises for input/penetration/exercising, etc. Supply references on disk if possible for inclusion in final report, AND HARDCOPY FOR SURE.)

Attempt Telnet through sniffer and observe autoshun occurs within 3 seconds.

Date/Time:(when tests conducted)

03/20/97 - 1518 hrs.

Alarm Level:

5

Location:(where tests orchestrated from)

National Security Agency (NSA)
DECIN Laboratory
FANX3
Room B4120

Participants:(who was present during tests)

Charles Freeman, V21

James Codespote, Y44

Linda Jessen, R23

Hardware Complement: (model/designations of major equipment used during tests)

Director - Sun SPARC 20
Target - Sun SPARC 5
Sensor - NSX
Routers (2) - NSC Border Guard 2000

Software Complement: (generic names of major software used during tests)

Director - Solaris 2.5
HP Openview - 4.11

Test Equipment: (Model/designations of major test equipment used during testing)

Protocol Analyzer - Wandel & Goltermann DA-30

Result Summary: (observer conclusions)

Match: IFS=/ icons appeared - alarm source 208.213.191.4, alarm source 144.51.132.98

caught both ways, coming in and echo back.

Verified time slot by using network analyzer.

Time on / is 15:19:29:00819

Time on last packet is 15:19:33:75427 (4.75 secs).

Claims: Verified based on average

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

38 & 39

Script Reference: (data files used during exercises for input/penetration/exercising, etc. Supply references on disk if possible for inclusion in final report, AND HARDCOPY FOR SURE.)

Configure NSX to log keystrokes form specified attack type.

Run attack and verify that keystroke capture occurs.

Date/Time:(when tests conducted)

03/20/97 - 1550 hrs.

Alarm Level:

5

Location:(where tests orchestrated from)

National Security Agency (NSA)
DECIN Laboratory
FANX3
Room B4120

Participants:(who was present during tests)

Charles Freeman, V21

James Codespote, Y44

Linda Jessen, R23

Hardware Complement: (model/designations of major equipment used during tests)

Director - Sun SPARC 20
Target - Sun SPARC 5
Sensor - NSX
Routers (2) - NSC Border Guard 2000

Software Complement: (generic names of major software used during tests)

Director - Solaris 2.5
HP Openview - 4.11

Test Equipment: (Model/designations of major test equipment used during testing)

Protocol Analyzer - Wandel & Goltermann DA-30

Result Summary: (observer conclusions)

Match: IFS=/ icons appeared - alarm source 208.213.191.4, alarm source 144.51.132.98

Alarm Name - String Match

NSX automatically created log file.

log files = IPlog.144.51.132.98 & IPlog.208.213.191.4 - create time 1555

Claims: Verified

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

15 & 16

Script Reference: (data files used during exercises for input/penetration/exercising, etc. Supply references on disk if possible for inclusion in final report, AND HARDCOPY FOR SURE.)

Verify Primary Comms Path and Disconnect.

Verify Secondary Comms Path.

Date/Time:(when tests conducted)

03/21/97 - 0945 hrs.

Alarm Level:

5

Location:(where tests orchestrated from)

National Security Agency (NSA)
DECIN Laboratory
FANX3
Room B4120

Participants:(who was present during tests)

Charles Freeman, V21

James Codespote, Y44

Linda Jessen, R23

Hardware Complement: (model/designations of major equipment used during tests)

Director - Sun SPARC 20
Target - Sun SPARC 5
Sensor - NSX
Routers (2) - NSC Border Guard 2000

Software Complement: (generic names of major software used during tests)

Director - Solaris 2.5
HP Openview - 4.11

Test Equipment: (Model/designations of major test equipment used during testing)

Protocol Analyzer - Wandel & Goltermann DA-30

Result Summary: (observer conclusions)

Pulled cable 144.51.132.97 from Director machine to test 144.51.132.129 line, port le0

Did ifconfig le0 down

COACT established telnet session w/director saw via NetAnalyzer

Did route delete 147.51.26.94, results returned: delete route host 147.51.26.94 gateway 144.51.132.125

Plugged in cable

Did ifconfig le0 up

Did route add 147.51.26.94 144.51.132.125, results returned: add host 147.51.26.94 gateway 144.51.132.125

Icom_IP_Spoof_Fail, 2, Icom_IP_Spoof_Fail, 13, & Icomp_UDP_Fail, 301 icons appear, also saw packets on net analyzer.

Extensive operator intervention needed to switch to alternate network path. This was due to routing problems in Solaris Operating System. In our opinion test was not truly verified because it was NOT automatic. Some amount of work needed if feature didn't function properly. However, when second path was manually established, communications resumed as before.

Claims: Verified

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

40 & 41

Script Reference: (data files used during exercises for input/penetration/exercising, etc. Supply references on disk if possible for inclusion in final report, AND HARDCOPY FOR SURE.)

Configure NSX to dump Event and IP Session logs to an archive device.

Verify that data has transferred to off-line device.

Date/Time:(when tests conducted)

03/21/97 - 1035 hrs.

Alarm Level:

No Alarm

Location:(where tests orchestrated from)

National Security Agency (NSA)
DECIN Laboratory
FANX3
Room B4120

Participants:(who was present during tests)

Charles Freeman, V21

James Codespote, Y44

Linda Jessen, R23

Hardware Complement: (model/designations of major equipment used during tests)

Director - Sun SPARC 20
Target - Sun SPARC 5
Sensor - NSX
Routers (2) - NSC Border Guard 2000

Software Complement: (generic names of major software used during tests)

Director - Solaris 2.5
HP Openview - 4.11

Test Equipment: (Model/designations of major test equipment used during testing)

Protocol Analyzer - Wandel & Goltermann DA-305

Result Summary: (observer conclusions)

Something was written to tape drive.

Claims: Verified

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

37

Script Reference: (data files used during exercises for input/penetration/exercising, etc. Supply references on disk if possible for inclusion in final report, AND HARDCOPY FOR SURE.)

Attempt Telnet through sniffer and observe autoshun occurs within 3 seconds.

Date/Time:(when tests conducted)

03/21/97 - 1041 hrs.

Alarm Level:

5

Location:(where tests orchestrated from)

National Security Agency (NSA)
DECIN Laboratory
FANX3
Room B4120

Participants:(who was present during tests)

Charles Freeman, V21

James Codespote, Y44

Linda Jessen, R23

Hardware Complement: (model/designations of major equipment used during tests)

Director - Sun SPARC 20
Target - Sun SPARC 5
Sensor - NSX
Routers (2) - NSC Border Guard 2000

Software Complement: (generic names of major software used during tests)

Director - Solaris 2.5
HP Openview - 4.11

Test Equipment: (Model/designations of major test equipment used during testing)

Protocol Analyzer - Wandel & Goltermann DA-30

Result Summary: (observer conclusions)

Retry from yesterday to see if we can get 3 seconds.

Match: IFS=/ icons appeared - alarm source 208.213.191.4, alarm source 144.51.132.98

caught both ways, coming in and echo back.

Time on / is 10:42:54:72

Time on last packet is 10:42:58:36 (3.64 secs).

Claims: Verified based on average

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

37

Script Reference: (data files used during exercises for input/penetration/exercising, etc. Supply references on disk if possible for inclusion in final report, AND HARDCOPY FOR SURE.)

Attempt Telnet through sniffer and observe autoshun occurs within 3 seconds.

Date/Time:(when tests conducted)

03/21/97 - 1053 hrs.

Alarm Level:

5

Location:(where tests orchestrated from)

National Security Agency (NSA)
DECIN Laboratory
FANX3
Room B4120

Participants:(who was present during tests)

Charles Freeman, V21

James Codespote, Y44

Linda Jessen, R23

Hardware Complement: (model/designations of major equipment used during tests)

Director - Sun SPARC 20
Target - Sun SPARC 5
Sensor - NSX
Routers (2) - NSC Border Guard 2000

Software Complement: (generic names of major software used during tests)

Director - Solaris 2.5
HP Openview - 4.11

Test Equipment: (Model/designations of major test equipment used during testing)

Protocol Analyzer - Wandel & Goltermann DA-30

Result Summary: (observer conclusions)

Retry Again

Match: IFS=/ icons appeared - alarm source 208.213.191.4, alarm source 144.51.132.98 caught both ways, coming in and echo back.

Time on / is 10:54:27:41

Time on last packet is 10:54:32:76 (5.35 secs).

Claims: Verified based on average

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

37

Script Reference: (data files used during exercises for input/penetration/exercising, etc. Supply references on disk if possible for inclusion in final report, AND HARDCOPY FOR SURE.)

Attempt Telnet through sniffer and observe autoshun occurs within 3 seconds.

Date/Time:(when tests conducted)

03/21/97 - 1058 hrs.

Alarm Level:

5

Location:(where tests orchestrated from)

National Security Agency (NSA)
DECIN Laboratory
FANX3
Room B4120

Participants:(who was present during tests)

Charles Freeman, V21

James Codespote, Y44

Linda Jessen, R23

Hardware Complement: (model/designations of major equipment used during tests)

Director - Sun SPARC 20
Target - Sun SPARC 5
Sensor - NSX
Routers (2) - NSC Border Guard 2000

Software Complement: (generic names of major software used during tests)

Director - Solaris 2.5
HP Openview - 4.11

Test Equipment: (Model/designations of major test equipment used during testing)

Protocol Analyzer - Wandel & Goltermann DA-30

Result Summary: (observer conclusions)

Retry Again

Match: IFS=/ icons appeared - alarm source 208.213.191.4, alarm source 144.51.132.98 caught both ways, coming in and echo back.

Time on / is 10:59:53:03

Time on last packet is 10:59:53:67 (.67 secs).

Claims: Verified based on average

SPAWAR (MITRE) REPORTS

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

Event 9 and 10

Date/Time: (when tests conducted)

1:32 pm, 3/19/97

Location: (where tests orchestrated from)

MITRE - Washington

Participants: (who was present during tests)

Tom Gregg
Lara Sosnosky
Manfred Reek

Hardware Complement: (model/designations of major equipment used during tests)
ERS Passport
Borderguard
NSX
Director

Major Events: (plain English dialog of events)

Change passwd spock97 to spock96 in nrConfigure window.
telnet to 205.1.30.`142.62 (NSX-SPAWAR)
looked at 'errors.managed" log file
(GUI did not work), manually edited 'managed conf" --->changed spock97 to spock96
restarted 'nr.managed'
rebooted at 'errors.managed--->verified wrong username/password
re-edited 'managed conf" --->changed spock96 back to spock97
killed nr.managed process --->restarted same process

Verified nr.managed NetDevice status was active through GUI

Result Summary: (observer conclusions)

GUI did not work when we tried to change the password from spock97 to spock96

It would be nice to have the Token Names in alphabetical order (in the nrConfigure window)

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

Event 19

Date/Time: (when tests conducted)

2:41 pm, 3/19/97

Location: (where tests orchestrated from)

MITRE - Washington

Participants: (who was present during tests)

Sandi Aguirre
Tom Gregg
Lara Sosnosky
Manfred Reek

Hardware Complement: (model/designations of major equipment used during tests)

ERS Passport
BorderGuard
NSX
Director

Major Events: (plain English dialog of events)

1. - saw incom1-tcp-fail alarms & TCP Port Sweep (red) alarm

2. - selected TCP Port Sweep

3. - applied '"shun" under security to ongoing attack from COACT IP address

4. - COACT verified shun timed out (shun set to 5 minutes)

Result Summary: (observer conclusions)

Recommendation: When SHUN is selected, user should be told when the SHUN will expire (after x minutes).

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

Events 22 & 23

Date/Time: (when tests conducted)

9:20 am. 3/20/97

Location: (where tests orchestrated from)

MITRE - Washington

Participants: (who was present during tests)

Lara Sosonsky
Sandi Aguirre
Manfred Reek
Tom Gregg
Gary Gagnon
Justin Tran

Hardware Complement: (model/designations of major equipment used during tests)
ERS Passport
Borderguard
NSX
Director

Major Events: (plain English dialog of events)

received multiple red & yellow alarms
deleted yellow alerts

-port sweep ran on different ports - not similar enough to consolidate high level alarms

-low-level (yellow) alarms <u>did</u> consolidate into single icon

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

Events 24 & 25

Date/Time: (when tests conducted)

10:09 AM

Location: (where tests orchestrated from)

MITRE - Washington

Participants: (who was present during tests)

Lara Sosnosky
Sandi Aguirre
Manfred Reek

Hardware Complement: (model/designations of major equipment used during tests)

ERS Passport
Borderguard
NSX
Director

Major Events: (plain English dialog of events)

Alarms	Name	From	Dest	Alarm Lev.
Received:	TCP Port Sweep	208 213.191.4	205.130.144.22	3

Source Port	Dest Port	Source port	Dest. Port
33142	1 (16 07 05)	33190	17
33145	2	33193	18
33148	3	33196	19
33151	4	33199	20
33154	5	33202	21
33157	6	33205	22 (16:07:05)
—>red alert - severity +5 sp=33157 dp=6		33172	11
33160	7	33178	13 (16:07:14)

33163	8
33166	9
{33169	10
{33175	12
{33181	14
{33184	15
33187	16

Result Summary: (observer conclusions)

Some lower level alerts were received "out of order" on our screen and we verified this by the time it was received.

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

Events 28, 29, 31, 32

Date/Time: (when tests conducted)

12:30 pm. 3/20/97

Location: (where tests orchestrated from)

MITRE - Washington

Participants: (who was present during tests)

Lara Sosnosky
Sandi Aguirre
Manfred Reek

Hardware Complement: (model/designations of major equipment used during tests)

ERS Passport
Borderguard
NSX
Director

Major Events: (plain English dialog of events)

Name	From	Dest	Time	Source Port	Dest. Port	Level
INCOM1-LOGIN-FAIL	208-213.191.4	205.130.144.22	18:37:39	1023	513	3
MAIL:recon (vrfy)	"	"	18:44:59	33294	25	3
INCOM1-TCP-FAIL	"	"	16:07:05	33142	1	3
"	"	"	16:07:05	33145	2	3
"	"	"	16:07:05	33148	3	3
"	"	"	"	33151	4	3
"	"	"	"	33154	5	3
"	"	"	"	33157	6	3
TCP-PORT-SWEEP	"	"	"	33157	6	5
INCOM1-TCP-FAIL	"	"	"	33160	7	3

"	"	"	"	33163	8	3
"	"	"	"	33166	9	3
"	"	"	"	33169	10	3
"	"	"	"	33175	12	3

Name	From	Dest	Time	Source Port	Dest. Port	Level
"	"	"	"	33181	14	3
"	"	"	"	33184	15	3
"	"	"	"	33187	16	3
"	"	"	"	33190	17	3
"	"	"	"	33193	18	3
"	"	"	"	33196	19	3
"	"	"	"	33199	20	3

Result Summary: (observer conclusions)

NOTE: Time on our machine is 6 hours ahead of actual time

NAME	FROM	DEST	TIME	SOURCE PORT	DEST PORT	LEVEL
INCOM1_FTP_FAIL	208.213 191 4	205.130.144.22	16:07:05	33202	21	3
INCOM1_TCP-FAIL	"	"	"	33205	22	3
"	"	"	16:07:08	33172	11	3
"	"	"	16:07:14	33178	13	3
MATCH : IFS=/	"	"	19:04:26	33300	23	5
"	205.130 144 22	208 213.191.4	19:04:26	33300	23	5

(MASTER) *locally reproduce as needed*

Interrogation forms Used During the NetRanger Exercises

REFERENCE EVENT NUMBER: (event log reference number.)

Event 36

Script Reference: (data files used during exercises for input/penetration/exercising, etc. Supply references on disk if possible for inclusion in final report, AND HARDCOPY FOR SURE.)

MITRE. McLean, VA

Date/Time: (when tests conducted)

3:00 pm. 3/20/97

Location: (where tests orchestrated from)

MITRE - Washington
Participants: (who was present during tests)

Lara Sosnosky
Sandi Aguirre
Manfred Reek

Hardware Complement: (model/designations of major equipment used during tests)

ERS Passport
Borderguard
NSX
Director

Major Events: (plain English dialog of events)

-received alert - "Match : 1etc/shadow"

-manually selected alert, choose "shun_source ip"

-COACT verified our "shun"

-manually chose 'unshun_source ip"

(in nrConfigure window:)
nr.managed ---> UnshunAll ---> nvexec

-COACT verified our 'unshun"

Result Summary: (observer conclusions)

Unshun under Security --->UnShun--->Source IP

does not work - had to unshun in nrConfigure window instead.

FOR OFFICIAL USE ONLY

SECURITY PROOF OF CONCEPT KEYSTONE

NETRANGER REAL-TIME NETWORK INTRUSION DETECTION
Performance and Security Test
Appendix C
Minutes of Proof of Concept Planning Meetings

Prepared for:
Maryland Procurement Office
9800 Savage Road
Fort George G. Meade, Md. 20755

Contract:
MDA904-96-C-0215

By
COACT, Inc.
9140 Guilford Road, Suite L
Columbia, Maryland 21046

Document No. 010511

30 April 1997

DISTRIBUTION STATEMENT Distribution of Appendix C is authorized to U.S. Government Agencies only. Refer other requests for this document to Director NSA, attn. NSA/V21, Fort George G. Meade Md. 20755.

Not relansable to the Defense Technical Information Center Per DoD Instruction 3200.12 Distribution limited to U. S. Government Agencies Only
This document contains NSA information (Jan.1992). Request for this document must be referred to the Director NSA.

FOR OFFICIAL USE ONLY

Appendix C

Introduction

This Appendix contains information related to the SPOCK (Security Proof of Concept Keystone) report on the WheelGroup NetRanger Real-Time Network Intrusion Detection Product.

Content. The following materials are presented in this Appendix:

1) Minutes of Proof of Concept Planning Meetings

Minutes of Proof of Concept Planning Meetings

There are three levels of engagement in SPOCK:

1) SPOCK membership and attendance at monthly meetings,

2) Briefing at forums (related to products, architectures, etc) that are security-based.

3) Submitting security claims on specific products, architectures, etc. for consideration by Consortium members, often resulting in proof-of-concept validation and SPOCK reports.

The minutes presented here resulted from such a process; they outline the processes followed for WheelGroup NetRanger from its inception to its completion. Furthermore, the minutes show that there was full participation by members of the Consortium throughout the entire process, including the testing events. For more information regarding the test scripts and the Event Logs used for testing, see Appendix A, Scripts Used During Testing. Form more information on the comments made by the participants during testing, see Appendix B, Participant Verification and Comments.

The minutes from the planning meetings have been sanitized, and all personal contact information regarding the participants has been removed to protect them from unauthorized contact. NSA V21 will coordinate any legitimate communication needs with the affected individuals. The distribution of this appendix is restricted to government activities with a legitimate need-to-know.

Conference Report
(spocmin1)

Minutes of SPOCK Meeting July 2, 1996

Date of Conversation: 2 July 1996

Personnel in Conversation: See page 3

OLD BUSINESS:

This meeting was held to discuss the future vision of the SPOCK program, present information on the NSA direction for the 21st century and discuss a commercial security product offering from WheelGroup.

The meeting was opened at 10:00 a.m. by Bill Marshall (chief NSA/V2) Attendees were introduced and the minutes of the June meeting were reviewed and approved with no changes.

NEW BUSINESS:

Mr. Giles clarified the purpose of the list of electronic products to be posted on the Intelnet and Internet. It is a general knowledge of products known to V2 and what types and levels of evaluation (if any) have been accomplished on each. It is not a list of SPOCK reviewed products. SPOCK reviewed products will be handled separately but may also be included in this previously discussed database, originally presented at the June 4 SPOCK meeting.

Mr. Marshall discussed the background and actions the NSA Director has taken to audit the Agency and gain insight to its activities towards developing a long term strategy. He focused particularly on the INFOSEC area and its improved position to communicate and participate with the commercial security community toward developing industry based and accepted solutions for all but the highest command/control government needs, (and possibly there as well in the future.)

PRESENTATIONS:

Two presentations were given. The first was by Mr. Lou Giles, NSA/V21 who is serving on a Director's tiger team to develop NSA's long term mission strategies. Highlights:

.mission development is for next 20 years
.working level input has been modified by Director
.information security superiority is Agency goal
.internal re-alignments will be accomplished to eliminate cross purposes
.main national threat is hacker penetration of national infrastructure, i.e. airline schedules, powergrid alignments, etc. NOT JUST INTERNET
.NSA involved solutions must accommodate law enforcement's legitimate interests
.Industry and govt. together must balance those interests.
.GOTS to COTS and/or COTS to GOTS security solutions open to Govt/Industry dialog
.Attacks are a fact of life. "Defense first, Validated strategic threat second" says the Director.
.In the future, NSA is for risk management vs. risk avoidance.
.Govt. uses "loss of life" security criteria and Private sector uses "insurance" with costs passed to customer (i.e placing a price on the lossses). These approaches must be merged.
.The *strategic threat* is NSA's jurisdiction.
.All the above encompasses the basis of NSA,s National Cryptologic Strategy for the 21st Century, known as *NCS21* e.g.:
1 set of standards for both civil and defense security interests

NIST/NSA/Industry to develop public key criteria. Industry to develop and supply the algorithms meeting the criteria.
Common Criteria program developed by seven countries plus NSA
functionality and assurance methods described
1 step profile developed from common criteria
Originators of Common Criteria looking to outside interests to execute the profile developments.
SPOCK complements Common Criteria
SPOCK is recognized and largely funded for FY97 under new NSA FINPLAN

Lou Giles and Bill Marshall extended an invitation to the forum membership to call for any assistance or discussion.

Lee Sutterfield representing WheelGroup gave a detailed analysis of their NetRanger "intrusion detection plus" product. They are a new company based on employees from the Information Warfare Center who are teaming with venture capital to commercialize their security solutions developed for the Air Force.
Highlights:
.operationally orientated solutions
.based on AF protection program
.two parts, Director and NSX
.essentially a computer based substitute for a human based security operations center
.NSX watches the store
.Director controls and watches NSX
.Remote monitoring of Operation available through Netsolve Inc. in Austin TX.
.Bottom line: technician deals with 80 per cent of the installation, setup and operation
WheelGroup advises backup engineering support (20 per cent).
.Products expanding and emerging
.SPOCK claims for a Proof of Concept anticipated in OCT/NOV timeframe.

The next SPOCK meeting is scheduled for August 6 at COACT facilities in Columbia Md. A *presentations* candidate list is being formulated for the next six months and *potential POCs* are being weighed in for resources required to *conduct solid broad based claims evaluations*. You may call Larry B. McGinness, COACT SPOCK Program Manager , or Terry Losonsky, NSA/V2 SPOCK Program Manager to discuss both subjects. Either way, we will coordinate with each other.

Conference Report
(spocmi21)

Minutes of SPOCK Meeting 4 November, 1996

Date of Conversation: 4 November 1996

Personnel in Conversation: See attachment.

BACKGROUND:

This meeting was held to discuss the WheelGroup NetRanger product, an intrusion detection software package residing on an NSC BorderGuard Router.

The meeting was opened at 1.45 p.m. by Terry Losonsky, NSA/V21.

DISCUSSION POINTS:

Terry Losonsky, NSA/V2 explained the relationship between vendor claims, SPOCK architecture, and the marriage to warfighter applications. He also explained our relationship with traditional SPOCK partners, i.e. NSA/Y4, C2, V2, and R2 plus Space Warfare Center, Battle Command Battle Laboratories, IRS, AFWIC, and COMPUCAT (aus.)

He explained SPOCK's relationship to AFWIC and the upcoming static test of NetRanger by them.

Robert Gooch, WheelGroup, explained the requirement for the Director (a monitoring station for NetRanger input and control):

> Workstation running HP Openview (manages over100 items), license cost aprox. $17k.
> or HP Node Manager (manages up to 100 items), license cost aprox. $4k.
>
> NetRanger Software (provided by WheelGroup during test.)
>
> Unix or Solaris x86 etc. Operating Software

The router hosting the NetRanger may be a BoarderGuard 1000 (256-512kb), or 2000 (T1 rate). 2000 preferred.

Three sites of NetRanger software can be provided. Four is possible with sufficient justification.

Setup requires input from the site in the form of a completed four page architectural survey.

Setup occurs during the first day with on-site engineering assistance from WheelGroup.

Operator training occurs during the second day.

Joint monitoring of the operational NetRanger during the third day is used to verify operation and adjust (tune the software for normal false positive alarms.) This means suppressing report generation, alarm reporting, or alarming at all.

Existing BoarderGuard Routers can be used to host NetRanger during the tests. The operational control of the router will shift to the security function and personnel during those tests however. (Suggested the same person responsible for the router daily operation also participate in the test.)

To prevent any penetration tests from becoming visible on the Internet, additional BoarderGuards can be used as sleeve encryptors to buffer the Internet from those conducting the penetration.

The architecture consists of NSC BoarderGuards acting as home to NSX and Director workstations.

The BoarderGuards are then homed to the Internet for connectivity between sites.

The participants suggested AFWIC run full attacks against NetRanger during the static tests.

Y4/V2 would run network attacks (SATAN, etc.).

ACTIONS:

WheelGroup will provide site hardware/software requirements and the Architectural questionnaire to COACT for coordination with the sites.

NSA/V2 will solicit information from the sites.

ADDITIONAL COORDINATION:

CPT Artiaga, or associates will travel on 11 November to one or more sites. WheelGroup was requested to make the action deliverables available in time for those TDY's.

Personnel in Conversation:

Terry Losonsky, NSA/V21
CPT Jay Artiaga, NSA/V21
Larry B. McGinness, COACT
Darwin Annala, NSA
Jim Codespote, NSA
Charles Freeman, NSA
John McIver, NSA/V2
Robert Gooch, WheelGroup

Conference Report

Minutes of SPOCK Meeting 4 November, 1996

Date of Conversation: 4 November 1996

Personnel in Conversation: See attachment.

BACKGROUND:

This meeting was held to discuss the WheelGroup NetRanger product, an intrusion detection software package residing on an NSC BorderGuard Router.

The meeting was opened at 1.45 p.m. by Terry Losonsky, NSA/V21.

DISCUSSION POINTS:

Terry Losonsky, NSA/V2 explained the relationship between vendor claims, SPOCK architecture, and the marriage to warfighter applications. He also explained our relationship with traditional SPOCK partners, i.e. NSA/Y4, C2, V2, and R2 plus Space Warfare Center, Battle Command Battle Laboratories, IRS, AFWIC, and COMPUCAT (aus.)

He explained SPOCK's relationship to AFWIC and the upcoming static test of NetRanger by them.

Robert Gooch, WheelGroup, explained the requirement for the Director (a monitoring station for NetRanger input and control):

> Workstation running HP Openview (manages over100 items), license cost aprox. $17k.
> or HP Node Manager (manages up to 100 items), license cost aprox. $4k.
>
> NetRanger Software (provided by WheelGroup during test.)
>
> Unix or Solaris x86 etc. Operating Software

The router hosting the NetRanger may be a BoarderGuard 1000 (256-512kb), or 2000 (T1 rate). 2000 preferred.

Three sites of NetRanger software can be provided. Four is possible with sufficient justification.

Setup requires input from the site in the form of a completed four page architectural survey.

Setup occurs during the first day with on-site engineering assistance from WheelGroup.

Operator training occurs during the second day.

Joint monitoring of the operational NetRanger during the third day is used to verify operation and adjust (tune the software for normal false positive alarms.) This means suppressing report generation, alarm reporting, or alarming at all.

Existing BoarderGuard Routers can be used to host NetRanger during the tests. The operational control of the router will shift to the security function and personnel during those tests however. (Suggested the same person responsible for the router daily operation also participate in the test.)

To prevent any penetration tests from becoming visible on the Internet, additional BoarderGuards can be used as sleeve encryptors to buffer the Internet from those conducting the penetration.

The architecture consists of NSC BoarderGuards acting as home to NSX and Director workstations.

The BoarderGuards are then homed to the Internet for connectivity between sites.

The participants suggested AFWIC run full attacks against NetRanger during the static tests.

Y4/V2 would run network attacks (SATAN, etc.).

ACTIONS:

WheelGroup will provide site hardware/software requirements and the Architectural questionnaire to COACT for coordination with the sites.

NSA/V2 will solicit information from the sites.

ADDITIONAL COORDINATION:

CPT Artiaga, or associates will travel on 11 November to one or more sites. WheelGroup was requested to make the action deliverables available in time for those TDY's.

Personnel in Conversation:

Terry Losonsky, NSA/V21
CPT Jay Artiaga, NSA/V21
Larry B. McGinness, COACT
Darwin Annala, NSA
Jim Codespote, NSA
Charles Freeman, NSA
John McIver, NSA/V2
Robert Gooch, WheelGroup

Conference Report
(spocmi23)

Minutes of SPOCK Meeting 30 November, 1996

Date of Conversation: 25 November 1996

Personnel in Conversation: See attachment.

BACKGROUND:

This meeting was held to discuss the Wheel Group NetRanger Proof of Concept.
The meeting was opened at 1.00p.m. by Terry Losonsky, NSA/V21.

DISCUSSION POINTS:

The Wheel Group representatives passed out a NetRanger high level overview to all present. They then briefed the attendees on the status of the NetRanger product. The bottom line is a new release is expected in December which will be fully functional and representative of the claims to be formally submitted.

CPT Artiaga provided coordination input from Battle Command Battle Laboratories at Ft. Gordon. They will not be available to participate until January 97.

Larry McGinness provided input from IITRI labs. (IRS). They will be unable to participate due to other commitments.

The attendees discussed a possible proof of concept timeframe. The 6 January timeframe was proposed because the host system (NSC NetSentry) will have completed their upgrade to release 4.0, while the NetRanger upgrade will also be completed to release 1.1.1.

Before the Proof of Concept can proceed, a network configuration and a list of proper equipment is needed, so the participants can acquire the necessary connectivity and tools.

A general discussion led to these conclusions:

AFWIC is currently conducting a bench test, including penetration exercises. 'Claims" could be made by Wheel Group and verified by reference to the results of the AFWIC report (provided the level of detail was sufficient to support the format and content requirements of the SPOCK reports.)

BTG can supply realistic data to run a simulation of warfighter applications during the exercise.

Four or five sensors, i.e. NSX's with BorderGuards are needed for the POC.

Proposed sites are AFWIC, BCBL, NSA, SWIC.

Two weeks would be needed to install and train site personnel before the commencement of the POC.

ACTIONS:
-A target date of 15-18 December is chosen for a follow on meeting.
-Wheel Group is responsible for proposing an architecture, with an accompanying security policy to be implemented at the sites. The product 'claims' will reflect the verification of that policy's effectiveness in maintaining operational integrity of the data flow with full security.
-Two NSC borderguards reside at IITRI. Larry and Terry will examine the possibility of moving them to NSA V2/Y4 for any proof of concept.

Personnel in Conversation:

Terry Losonsky, NSA/V21
CPT Jay Artiaga, NSA/V21
Larry B. McGinness, COACT
Gerry Lathem, Wheel Group
Todd Schell, Wheel Group
Bob Gleichauf, Wheel Group
Robert Gooch, Wheel Group
Tim Collins, BTG
Larry Phillips, BTG
Fred Schroeder, BTG

Conference Report
(spocmi26)

Minutes of SPOCK Meeting 16 December, 1996

Date of Conversation: 12 December 1996

Personnel in Conversation: See attachment.

<u>OLD BUSINESS</u>:

This meeting was held to discuss the status the WheelGroup NetRanger Demonstration/Test, review the actions underway by WheelGroup and BTG Inc., and determine what actions are needed by everyone else involved in the Demonstration.
The meeting was opened at 10.15 p.m.. by Terry Losonsky, NSA/V21. Larry Phillips, BTG, provided a DRAFT of a proposed implementation schedule and possible product claims.

<u>NEW BUSINESS:</u>

BTG requested a point of contact at Space Warfare Center. Terry gave them Col. Ben Hunsuck.

BTG announced Larry Phillips would be coordinating the product installation at AFWIC and SWC.

Tim Collins of BTG would handle FANX and Land Information Warfare Agency at Ft. Belvoir.

BTG expressed a desire to limit training of other contractors on their product during the test to limit.cost and exposure of the emerging product. They understand the resulting test will be made available to all requesters.

WheelGroup expressed a strong desire to focus on its' product's evaluation by eliminating such variables as the use of the R5 Passport Switch, which may complicate the demonstration.

BTG prefers T3 lines (vs. T1) between Ft. Belvoir and NSA.

WheelGroup stated that the demonstration must accommodate multiple security policies. Their experience indicates each service requires it's own unique policy for protecting their environment. Additionally, each site must be tailored to reduce/eliminate false positives.

The possibility (probability) of aseparate report from AFWIC was discussed. BTG strongly expressed the opinion that the SPOCK report must stand alone. They suggested random 'samples' (i.e. duplication) of some portions of the AFWIC tests be conducted by SPOCK to verify the accuracy/repeatability of the tests, but the content be repeated, not referenced, to the extent necessary to isolate the SPOCK report.

BTG expressed the desire that the SPOCK report, likely to be published after the AFWIC effort, build on the AFWIC exercise.

Larry McGinness, COACT, faxed the DRAFT calendar (implementation schedule) and DRAFT claims to WheelGroup who was participating in the conference via. phone.

The whole group then reviewed the claims and schedule. The consensus was to reduce and combine the claims, concentrating on those that differentiated NetRanger from like products, setting the high watermark for other products to measure against.

BTG pointed out that the reporting function of NetRanger was not suitable for examination as such because the reporting mechanism consists of third party vendor 'tools'. WheelGroup has qualified several of these products, and all NetRanger installed sites have successfully acquired/adapted software to adequately provide that function.

BTG stated it would take them at least three weeks to identify and supply any equipment lacking at the sites critical to the demonstration/test.

BTG stated their intent to demonstrate/test the 1.2 version (vs. 1.1.1) of NetRanger, with the latest enhancements.

The conferees reviewed the site complement. We have four sites participating. It was decided that five sites would be ideal.

The conferees determined they would need a minimum of 100 megabytes of warfighter compatible source test data plus suitable alarm generators (scripts) for the demonstration. BTG is looking into that problem. AT&T has supposedly conducted a 100 megabyte test on the product to determine NetRanger transparency to the AT&T data stream. The results were verbally passed to WheelGroup. (Larry has subsequently contacted AT&T but they cannot identify this effort. Larry Phillips has been contacted by Larry McGinness, and if BTG can supply Curt Jacobs the name and location of the test, Curt will try to gain permission to reference it, borrow the file used, or whatever. 16 Dec, LBM)

The conferees reviewed the minimum hardware needs for the demonstration.

SUMMARY:

BTG/WheelGroup have a better feel to clarify and simplify their claims.

They also have a better handle on hardware needs at the sites, scheduling issues and realistic benchmarks, etc.

Bottom Line: There is a window of opportunity to conduct this demonstration which needs everyone's undivided attention to close. The current scenario calls for January to stage everything to conduct the tests, including writing the security policies, training the participants, testing the lines, etc. Then, February is devoted to conducting the tests and beginning the creation of the SPOCK report.

Personnel in Conversation:

CPT Jay E. Artiaga, NSA/V2
Terry Losonsky, NSA/V2
Larry Phillips, BTG
Tim Collins, BTG
Robert Gooch, WheelGroup
Jerry Lathem, WheelGroup
Todd Shell, WheelGroup
Bob Glycof, WheelGroup

Conference Report
(spocmi29)

Minutes of WheelGroup NetRanger Script Writing Meeting 13 January, 1997
Date of Conversation: 7 January 1997
Personnel in Conversation: See attachment.

OLD BUSINESS:

This meeting was held to discuss the status of the WheelGroup Proof of Concept and determine what actions are necessary to move it forward.

The meeting was opened at 1.30 p.m. by Terry Losonsky, V2.

NEW BUSINESS:

The participants reviewed the draft claims and schedule worked out by BTG/WheelGroup.

The training being offered by WheelGroup in San Antonio was discussed. Attendees for the course were selected and arrangements made to brief those not attending prior to their participation in the POC. The course will be free, but the participants must pay room and transportation.

It was determined the Security Policy to be used for the POC should be written by the students after they fully understood the tradeoffs as a result of the training. The scripts would follow the security policy.

BTG needs input from each participating activity on their hardware/software inventory. Specifically, each site needs a proper workstation;, sufficient memory, and a dedicated NSC Borderguard Router.

One claim requires access to a full, unchanneled T3 line to test the transparency of NetRanger in high traffic flow situations.

The Navy may have a TAC3 line into NSA.

Claim 1.3: The participants discussed the possibility of demonstrating that the NetRanger could be configured to shut down a system input while NOT generating a report, to speed up response time.

The Participants discussed the possibility of demonstrating a feature whereby an internal table is created for Peacetime Reports, Shuns, etc., while a second table is configured for wartime applications. The NetRanger could then be re-configured quickly to match parameters with different emphasis and operating characteristics.

The participants discussed the possibility of demonstrating a feature whereby ALL reporting is shut down ONLY WHEN a 'volume' attack occurs. This would prevent the system from being flooded and causing NetRanger to effectively deny data throughput to its clients.

AFWIC wished to assure that the POC participants were aware, and the final report reflects, that NetRanger only protects UNIX systems.

Finally, the participants exchanged their E-mail addresses and phone numbers and agreed to directly exchange information within the group to expedite the proof of concept to adhere to the schedule.

ACTIONS:

All to respond to the following and provide feed back to Larry Phillips:

Do you have an HPWS that can be dedicated to the evaluation?

Do you have access to a T3 line that could be used for a short period of the evaluation?

Do you have access to the Internet?

Do you have a Border Guard router that can be used with the NetRanger Director?

ATTENDEES:

Jim Codespote, NSA
Mike Saft, NSA/R2
Jay ArtiagaNSA/V2
Darwin Annala NSA/Y44
Victor Hernandez, AFIWCIEASM
Terry Losonsky, NSA/V2
Charles Freeman, NSA/V2
Larry Phillips, BTG
Larry B. McGinness, COACT

Conference Report
(spocmi35)

Minutes of SPOCK Meeting
Date of Conversation: 28 January 1997
Personnel in Conversation: See Attachment

January 29, 1997

BACKGROUND:

This meeting was held to discuss Naval Research Labs participation in the Wheel Group Net Ranger Proof of Concept..
The meeting was opened at 1.00 p.m. by Larry McGinness, COACT.

DISCUSSION POINTS:

Larry explained to the NRL Representative the nature and history of SPOCK and NRL's previous involvement in the program.

He reviewed the S:POCK directory with NRL, demonstrating it's depth and breadth.

NRL explained their current task within the Center for High Assurance Computer Systems, namely to evaluate intrusion detection options.

Larry explained for the record that Larry Phillips had been contacted, informed of NRL interest in witnessing the POC, and Larry had requested permission to release to the NRL representative all background data leading up to the current level of development.

NRL stated for the record, they had contacted Lee Sutterfield and been referred to COACT. Further, the NRL representative will attend the 'Net Ranger school', albeit not the version currently underway for SPOCK participants.

The minutes of Wheel Group related meetings, latest architecture, claims, draft scripts, etc. was reviewed by NRL. All questions were explained by COACT satisfactorily. Copies were supplied for use by the NRL representative. Larry suggested 'immediate' coordination within the NRL security office, limited to government personnel only was prudent.

ACTIONS:

The NRL representative agreed to join the SPOCK forum on a permanent basis. His name has been added to the SPOCK directory. He will attend the February 4th meeting. He, and possibly others in his group will participate in the demonstration, functioning out of the COACT monitoring facility. This will provide them recognition within the resulting report.

Larry Phillips, BTG has been informed of the results of this meeting. He planned on attending, but had other commitments.

ATTENDEES:

Larry B. McGinness, COACT

Douglas R. Steinbaum, Center for High Assurance Computer Systems

Conference Report
(spocmi38)

Minutes of SPOCK Meeting February 6, 1997
Date of Conversation: 5 February 1997
Personnel in Conversation: See Attachment

BACKGROUND:

This meeting was held to discuss the status of the Wheel Group/BTG NetRanger Intrusion Detection proof of concept demonstration.
The meeting was opened at 1.30 p.m. by CPT Jay Artiaga, NSA/V2.

DISCUSSION POINTS:

Jay had prepared a handout containing pertinent information on security policy, architecture, and equipment delivery schedules. He briefed this to the group.

The 14th of February was selected by the group as a final script writing session prior to actually conducting the proof of concept in March.

Highlights:

17 to 21 February is slated for hardware delivery to the sites by BTG.

Operators documentation is being created by Wheel Group and is needed by the demonstration participants.

The SPAWARS group from the NAVY has expressed interest in participating in the demonstration. They have designated MITRE in Vienna as their arm to execute their portion of the exercise.
A meeting with MITRE/SPAWARS is scheduled for 7 February at MITRE.

The additional time to finalize configurations and arrange for equipment identification and delivery is the justification by the group for sliding the demonstration from late February to mid March.

BCBL participated in this discussion via telcon. BTG and BCBL discussed and resolved many connectivity and technical issues.

A proposal was made by BTG to move the proposed COACT monitor/attack launch equipment to the NSA/V2 lab to facilitate communication with the other sites. BTG mistakenly believed COACT only had Internet access via a modem connection. The NSA representatives raised some recent legal issues and latest guidance which led them to believe permission to operate from NSA would be difficult to obtain.

It was determined four NSC 2000 routers, equipped for ethernet would be needed for the LIWA, BCBL, MITRE, and COACT sites.

NSC requested details on the process to be used during the demonstration to coordinate and acquire documentation of the events.

COACT /BTG explained event logs would be used to assure participants were tracking and signing off on the scripts as they are conducted. Associated machine generated reports , logs, etc. will be tagged to each event sequence number and collected in envelopes for subsequent forwarding to COACT. The data will then be correlated.

The sites will be kept informed via telephone. E-MAIL summary statements will be sent periodically from the sites to COACT for the purpose of date/time stamping completion of key phases, etc.

BTG explained the rationale for needing multiple workstations as destinations for some claims verifications. The attendees agreed to identify and feed back information to BTG on this matter.

BTG announced they would add a sequence of scripts to the repertoire addressing common hacks as described by Becky Bace, Los Alamos Labs, in a recent SPOCK forum presentation. After some discussion, all agreed on the value of accomplishing this agenda. The importance of the company being able to accommodate any of these hacks within their database (should they successfully avoid detection) was deemed important to everyone at this meeting.

ACTIONS:

Larry Phillips will follow up with Wheel Group to assure Operator Documentation is sent to each participant (assumed to be the attendees at the recent Wheel Group training course in San Antonio.)

Additionally, he will provide the attendees and COACT with a philosophical addendum to the default security policy, implemented in the form of activated signature filters and alarm levels. This addendum is to provide insight on the rationale for selecting those particular filters and sensitivity levels.

Larry Phillips to arrange a meeting with MITRE to discuss involvement of Navy in the demonstration. Members of this group will also be invited.

BTG to arrange for hardware delivery during 17-21 February.

NSA/COACT to host script writing session at COACT on 14 February.

COACT to resolve ISDN connection requested by Larry Phillips for monitoring/attack facility at COACT for demonstration.

ATTENDEES:

Jay Artiaga, NSA/V2
Terry Losonsky, NSA/V2
Russell Dwire, NSG (NSC)
Manfred Reek, NSG (NSC)
Linda Jessen, NSA/R23
Doug Steinbaum, NRL-5541
Larry Phillips, BTG
Lt Charles Freeman, NSA/V2
Tim Collins, BTG
Jim Codespote, NSA
Daniel W. Fitzpartick, Sr, ACERT
Jack Deasy, LIWA
Larry B. McGinness, COACT
by teleconference:
Ray Casella, BCBL
LCDR Randy Sousa, SPAWAR/PMW161

Conference Report
(spocmi39)

Minutes of WheelGroup NetRanger Final Script Writing Meeting. 18 February, 1997
Date of Conversation: 14 February 1997
Personnel in Conversation: See attachment.

OLD BUSINESS:

This meeting was held to discuss the status of the WheelGroup Proof of Concept , complete the hardware arrangements, finalize the vendor claims, and complete the scripts the forum will use to verify those claims.

The meeting was opened at 10.25 a.m. by CPT Jay Artiaga, NSA/V2.

NEW BUSINESS:

Jay presented the group the agenda for the meeting:

Formally accept the Vendor's final Claims.
Formally review, modify, and accept the scripts to be used to verify those claims.
Finalize the hardware/software needs for each site, configuration details, and installation arrangements.
Discuss the legal implications of the proposed verification sequence, and arrangements to resolve them.

Larry McGinness, COACT, expanded on Jay's agenda. Specifically, the group was informed that they must concur on the draft scripts, created and adjusted over several previous meetings and fully verify the claims as they exist. If not, they must add additional scripts to adequately cover them, or the vendor must reduce the scope of the affected claims. Bottom line - this is the final script and claims conference. Based on past SPOCK proof of concept precedence, after today, no adjustments by either the vendor or forum will be entertained.

Larry Phillips, BTG and teleconfrees from WheelGroup, and BCBL, verified their hardware complement for the BCBL site.

Then, Larry verified the hardware/software complement with those present in the group. The NSA router will be upgraded by NSC for the test. A network analyzer will be loaned to them for the test.

Larry addressed his E-Mail to all participants asking them to have their IP addresses available for the meeting . BCBL, present by teleconference said they would E-Mail their addresses for their Router, Director, and Target Workstation. (5 addresses are required for each site.)

The participants received a replacement 'Default' list (list of implemented NetRanger filters and Alarm levels) to replace the ones they obtained during training. Additional detail has been provided explaining how the default alarm levels were arrived at. They also received a 'cloud' picture showing connections for the virtual net to be used during the test. (Copies were faxed to BCBL).

Larry clarified that for purposes of formal claims discussion, the word 'event' is synonymous with 'alarms'.

After a review of the default configuration and some discussion on the various levels of alarms to be used for verification (levels 3-5 are automatically sent from an NSX to a Director), a technical question was raised from AFWIC on the advisability of transmitting level 1 and 2 alarms to the monitor position at COACT. i.e. 'flooding' of the bandwidth could occur from network triggers (false positives) which occur normally. Larry stated that the risk was acceptable so the network could be observed from the launch point of the scripts and to adequately verify event/response and any external influences which may surface during the exercise. He said ONLY the monitor would be affected, not the launch vehicle (UNIX workstation) portion of the COACT installation.

BTG then referenced the spread sheet provided to the group. Claims are listed on the left, Scripts across the top, and X's within the matrix explain which scripts verify which claims. There is room to add participants for each script at the bottom. (This model has been used in other SPOCK proofs of concept to determine if all claims have been addressed, and if any extraneous scripts, not related specifically to claims verification are included in the test.

The test is divided into three parts. Static network configuration is a section of claims which will automatically be verified during pre-test of the virtual network. Phase 1 required the operators at the sites to take some action between each script. Phase 2 is not orchestrated in lock step with each site. Rather, scripts will be launched from the control center at COACT over a 30 minute period, using pre-canned attacks. The sites will merely verify the occurrence of the events , record the time and alarm conditions, and respond via E-mail to COACT 'for the record'.

The group discussed 'flooding' the NetRanger and other types of 'esoteric' attacks, protection from which is not addressed in BTG claims for the product. BTG's position is, based on prior SPOCK rules of engagement, testing by the group 'off the record' for these types of concerns are acceptable to BTG provide they occur after the formal claims have been verified, any negative results are provided to BTG for corrective action, and negative information is NOT included in the SPOCK report. They have no problem in the forum documenting the results in the form of minutes to share with the participants of the tests.

AFWIC and WheelGroup arrived at a standard configuration for both Bridge and Router configurations for use during the test.

ACTIONS:

These changes are to the claims/scripts document reviewed by the group at the meeting. BTG accepts responsibility for revising it according to the following comments from the group:

Phase I claims/scripts:

Claim 1.6 will be re-written to reflect that the referenced 'action' can only occur via an encrypted channel.

Claim 3.2.3 will be revised to change the reference to 'minimize' to reflect new wording to read: 'consolidate up to ## (number to be supplied by BTG) of alarm inputs into a single ICON.

Claim 3.2.4 will be changed to reflect consistent wording between the claims/scripts document and the spreadsheet. Specifically, the words 'marginal' and 'alarm level' present difficulty to the group in consistent claims identification. The words shall be 'merged' by BTG to reflect a consistent understanding of the terms.

Claim 1.1.3.1 will reflect the procedure 'attempt R-Login' from the same machine, outside the network. The second procedure referenced in the Claims/scripts document is considered redundant by the group and will be deleted from the test.

Claim 1.2.1.2 is designed with four procedures to reflect an 'atomic' signature (i.e. ping alarm). When all ports are subsequently swept, the alarm will reflect a composite event. After this discussion on the meaning of the terminology of atomic and composite signatures and the same event (ping) creating both types of alarm from an apparently single event, the group concurred with the claim and scripts. No changes are required to either.

Claim 1.3.2. is clarified to reflect that the never-shun IP list is effectively a 'trusted' list, because of the actions taken by NetRanger when automatically using the list as a reference source. BTG explained to the group that the administrator can always manually shun any IP address. With this clarification, no changes to the claim or scripts is required.

Claim 3.2.1. Delete the word 'complete' from the claim.

Claim 3.3. The 'pager' output is clarified to reflect 'alpha-numeric' capable. (The scripts will reflect an alpha-numeric test with FIWC and numerical test with NSA.

Three copies of the new 'Users Guide" to be shipped directly to each site by BTG.

Those sites using the Bridge configuration will need to supply NETMAP addresses in addition to the IP addresses.

Claim 1.4. FIWC and LIWA have volunteered to re-configure the severity of the alarms . The group agreed that two sites would be sufficient to verify this claim. The action of limiting this exercise to only two sites will reduce the coordination effort previously required to interface with all six sites during the test.

Claim 1.5. NSA and SPAWAR volunteered to participate in this script. Same rationale as Claim 1.4 applies.

Claim 1.6. NSA and LIWA volunteered to participate in this script. Same rationale as Claim 1.4.

Claim 2.1. AFWIC and FIWC volunteered to participate in this script. Same rationale as Claim 1.4.

Claim 2.1.2. NSA alone will participate in this script. The group agreed the complexity of dual-homing the site warranted the limitation to only one site to verify this claim.

Claim 3.1.2. NSA will re-configure LIWA and BCBL default configuration while FIWC will re-configure SPAWARs to verify the capability to remote out securely, the management of a given system when permission to do so has been granted by the affected system administrator. Upon verification of the changes, the original configurations shall be restored.

Claim 3.2.2. AFWIC, NSA, and BCBL shall participate in this script.

Claim 3.3. NSA and FWIC will verify this claim on pager notification. (see discussion section for details.)

Phase II Claims/scripts:

Claim 3.4. AFWIC will verify this claim by exercising the script (i.e. stages data to a RBDMS).

Claim 1.7. NSA and FIWC will verify this claim. (i.e. backing up the data by dumping to a hard drive while NetRanger continues to function.

Note: On Claims not specifically referenced in these minutes, all six sites will participate.

Schedule Actions:

Training on 25 March for Navy in San Antonio (WheelGroup).

Equipment to be configured and delivered before 3 March.

Validation to begin on 10 March.

ATTENDEES:

Jim Codespote, NSA/Y44
Jay Artiaga NSA/V2
Victor Hernandez, AFIWCIEASM
Terry Losonsky, SPOCK- PM
1LT Charles Freeman, NSA/V2
Larry Phillips, BTG
Larry B. McGinness, COACT
Linda Jessen, NSA/R23
Doug Steinbaum, NRL/5544
Cris Jordan, ACERT/CC
Michelle Pagan, ACERT
John Deasy, LIWA
LCDR Randy Souza, SPAWAR
Lt. Nina Kenmore, FIWC
Gary Gagnon, MITRE/SPAWAR

by teleconference:
Ray Casella, BCBL
Todd Schell, WheelGroup

NetRanger
Proof of Concept
(spock4)
Initial Claims Analysis and Test Development

Date: 14 February 1997

Meeting Location: COACT Inc.

Attendees: TBD

Agenda: Review Wheel Group/BTG POC *format*

Review it's content *depth & breadth*.

Discuss selection of test bed and participants (*when* in the process identified, *how* selected)

Discuss the *process* used to develop it's test and produce the final report.

Quantify the results of the discussion :

Claims refinement: (test *statements*)

Sub-element identification (i.e. test *measurement* criteria)

Sub-element processes (test *procedures*, *equipment*, *key* personnel)

Test Bed Architecture and Verification (finalizing *participation* and equipment *availability*)

Schedule Development & Coordination

Identification of Key Personnel & *Functional* Responsibility

Production of Final Test Plan

sub-element test list

names/*phone numbers*/coordination channels

location of test equipment and test data source(s)

Final Approval (what level and how soon)

Contingency Plans (re-group scenario)

NetRanger Test Development

Inputs for the Discussion from
COACT SPOCK PM

1. NetRanger Claims can fall in three general areas:

    Security goodness, i.e.
    encryption
    access control
    performance

2. Sub-elements to claims must be expressed in measureable terms, i.e.
    yes/no
    min/max
    within/between, etc.

3. Sub-elements, once identified must be directly linked to a POC response, i.e.
    procedures to measure
    test equipment/lashups

4. The *proposed* test bed is highly linked to the sub-elements. It is best to create a *script*, i.e.
    players and locations
    simulated/ real life data, representing actual/proposed product applications
    cost/benefit tests, i.e short clear exercises, in a timely manner.
    weigh follow-on/expansion of scripts against costs of loaned products and continued use of expertise.

5. Screen each sub-element for anticipated/possible result, i.e
    test will give some *definite result*, preferably *yes or no*. (*either* answer has positive value *if handled right*.
    each sub-element *must be attempted once adopted*, i.e. we <u>will report</u> *what we know*. any results will be put in context.
    test results can be summerized in *sub*-context and *overall* context, i.e. what do the facts mean in context of *this product vs. its peers* and *the product's function in overall security architecture.*

6. USE NSC Report as *the* GUIDE! It has set the SPOCK *standard* for conception, discussion, participation, documentation, and quality results that both govt. and industry *apparently value highly*.

L.B.M.

Conference Report
(spocmi42)

Minutes of WheelGroup NetRanger Final Script Writing Agency Review. 4 March, 1997
Date of Conversation: 3 March 1997
Personnel in Conversation: See attachment.

OLD BUSINESS:

This meeting was held to discuss the .of the WheelGroup Proof of Concept , the attacks to be launched, procedures to mitigate risk, and coordination to obtain legal release from the participants
The meeting was opened at 2.00 p.m. by Terry Losonsky, NSA/V2.

NEW BUSINESS:

Terry explained the purpose of this meeting, namely to share with invited participants the background of the proof of concept demonstration, the nature of the scripts/procedures, and the risks of launching these scripts over the Internet as viewed by the forum members.

BTG passed out a slightly revised packet of information similar to that used at the last script writing meeting. They then explained:

The exercise is to prove claims can be dynamically validate across an Internet system.
The package passed out includes 'bubble' configurations to be used during the test.
It also contains the details of the procedures for launching each scenario.

WheelGroup stated only the TELNET and SENDMAIL scenarios are even remotely 'invasive'.
The balance are primarily 'ping-sweeps' which fall within the legally allowed area known as network reconnaissance.

AFWIC was then added to the conference by pre-arranged Telecon. Lt. Ibanez, representing Victor Hernandez, the participant during the script generation sessions verified:

AFWIC is indeed familiar with all planned scenarios, having previously worked with Wheel Group during laboratory verifications of their effectiveness.
They will review the script 'tools' prior to the actual test.

COACT added that FIWC was also familiar with the scenarios from their previous exposure to the product, and had agreed to review the 'tools' as well.

BTG and WheelGroup discussed the possible methods of creating and launching the scenarios:

By 'fully canned' (including IP addresses) files.
By using the tools with 'flexibility' , with observers to verify by double checking the IP addresses prior to launching each script. They pointed out some of the 'tools' are dynamically interactive with the target and not conducive to 'canning'.

The NSA legal representatives and the attendees discussed the need and value in obtaining the concurrence of DDI prior to conducting this exercise.

The participants basically agreed with the checks and balances to be employed. The legal representatives recommended a release be obtained from those participating within NSA, using the pattern they recommended for the rest of the participants external to NSA. A briefing would be created to accompany the release to those who will sign off.

ACTIONS:

NSA/V2 will prepare the briefing for Agency management.

BTG/WheelGroup will coordinate with AFWIC and FIWC to discuss the specific 'tools' to be used and obtain their concurrence.

ATTENDEES:

Jim Codespote, NSA/Y44
Jay Artiaga NSA/V2
Lt. Ibanez, AFIWCIEASM (by phone)
Terry Losonsky, SPOCK- PM
1LT Charles Freeman, NSA/V2
Larry Phillips, BTG
Larry B. McGinness, COACT
Linda Jessen, NSA/R23
Jerry Lathem, WheelGroup
Chris Goggans, WheelGroup
Russell Dwire, NSG
Bob Moylan, StorageTec, NSG
Manfred R. Reek, NSG
Patricia A. Zaccari, NSA/C22
Ken Olthoff, NSA/V2
Robert Gooch, WheelGroup
Alonzo Robertson, NSA
Paul Kominos, NSA

Conference Report
(spocmi46)

Minutes of WheelGroup NetRanger Proof of Concept Execution. 24 March, 1997
Date of Conversation: 19-21 March 1997
Personnel in Conversation: See attachment.
Reference: NetRang4.xls file, 'Event Log'.

OLD BUSINESS:

This meeting was held to discuss the execution of the WheelGroup Proof of Concept , complete the hardware connectivity, and assign tasks during its orchestration.
The meeting was opened at 8.00a.m. by Larry B. McGinness, Coact.

NEW BUSINESS:

COACT briefed Terry Losonsky, NSA/V2 on the status of the arrangements for the proof of concept. This consisted of the following topics:

Sites brought up and those still being troubleshot.
The phone bank, established to coordinate with the sites, and the programming of the site's numbers.
The procedures and documents to be used to verify the IP addresses during each event.

Current remaining problems were FIWC connectivity with COACT, and loading SUN Solaris OS into the SPARC 5 loaned by NSA/V2 to COACT (the launch terminal for scripts). A proposed solution to the SPARC problem is to have WheelGroup use their LapTop instead of the SPARC 5.

COACT discussed with WheelGroup the capability of the SPARC20 (monitor terminal) to take snapshots of the monitor screen as events unfolded. It was decided to use the audit log instead (for inclusion in the report), with illustrations from the manuals to show typical types of screens. (This decision had to do with reproduction quality in the reports. The manual illustrations were adjusted for resolution and contrast to be suitable for reproducing.)

Terry Losonsky returned to NSA to brief the DDI for permission to execute the proof of concept.

A sign-in sheet was begun for the attendees/participants.

At 0905, FIWC problem was isolated to a firewall filter, needing local authority to remove.

ACTIONS:

Reference WheelGroup Scripts and Master Event Log (with events referenced to scripts):

COACT maintained the Event Recording of time of launch, and monitored conversations over the phone bank.

BTG manned the Phone Bank, coordinating with sites.

WheelGroup launched the attack scripts, using the laptop, connected via ISDN 64kbyte through the internet, to the sites, and monitored/communicated with the NSX/Directors using the SPARC 20. Also provided technical support when requested over the phone banks.

NSA/V2 monitored the IP addresses before each launch, and maintained the Master set of observation forms, recording key information on each event.

Event 1 - (1300) A potential 'problem' occurred in verifying the claim that NetRanger can be deployed as a bridge or router.
The scripts to verify this claim were based on using ping sweeps (strobe) attack. It was discovered that some sites in 'bridging' mode would not respond to the pings. We determined that NetSentry is configured (actually the normal architecture of Ethernet) so that non-existent targets, i.e. non-connected equipment, don' t respond with a ping. As the NetRanger ping sweep signature is created to only recognize six or more pings as a ping sweep, and ethernet protocol only provides pings for existing connected hosts, only sites with six or more hosts will trigger the signature alarm *in bridging* mode.

As FIWC did have the requisite hosts, and was also configured in bridging mode, the claim was verified using the pre-arranged scripts for event 1. However, alternate signatures, not requiring six pings, were used at the other bridge sites to verify the claim.

Events 2 - 6 (1305) These are verified by virtue of the existence of the established, functioning network. All sites connected and functioning except BCBL, which is having trouble getting to LIWA and NSA The specific symptom is periodic loss of the encrypted sleeves. The BCBL to COACT connection is better, but not perfect. Our analysis attributes their difficulty to a 256kbyte pipe, being shared by BCBL with the rest of the base, while the other players have T1 connectivity.

Event 7 - (1330) verified.

Event 8 - (1332) verified

Event 9 - (1345) verified

Event 10 - (1350) verified.

Event 11 - (1400) verified

Event 12 - (1405) verified

Event 13 - (1415) verified

Event 14 - (1415) verified

Event 15 - bypassed.

Event 16 - bypassed.

Event 17 - (1420) verified

Event 18 - (1430) verified

Event 19 - (1435) verified

Event 20 - (1500) attempted but not verified.
Event 21 - (1505) attempted but not verified.

End of session for Wednesday, 19 March 97.

Beginning of events for Thursday, 20 March 97.

A review of residual problems from Wednesday:

COACT site not able to TELNET to NSA site. The NSA has a sniffer on the line and is able to read the TELNET packets coming in. NSA has tried to TELNET to themselves to no avail. All assume the NSA system administrator has not enabled proper protocol (50 or 60), this being an NSA action.

The BCBL host is still locking up. The problem has been further isolated to the rented SPARC terminal, which apparently has insufficient memory. (WheelGroup notes that the partition on the disk was reviewed, and although not as large as usually used with their product, they assumed it would be sufficient for the test. Apparently, the memory is being eaten up more than anticipated. WheelGroup is freeing up memory by eliminating superfluous HP OpenView functionality, and clearing out some of the audit log.

Also found an IP error (NSX to Director), which has been corrected.

Events 20 and 21 remain unverified. WheelGroup has reviewed the problem and conveyed software changes to COACT site. The tests can now be re-run.

Event 20 -(0905) repeated and verified successfully.

Event 21 - (0915) repeated and verified successfully.

Event 22 - (0935) verified.

Event 23 - (0930) verified.

Event 24 - (0940) verified.

Event 25 - (0942) verified.

Test halted to troubleshoot the COACT Sparc 5 disk drive, needed to load the SOLARIS OS. This terminal will be needed for phase 2 tests to launch SATAN scripts.

(1230) SPARC 5 up and loaded with SATAN as obtained from the Internet. This version requires the user to register on Domain Name Server. BTG System Administrator contacted and COACT site registered under BTG administration. As NetRanger network was brought up so rapidly, no sites are registered on DNS. Hence, SATAN will not operate.

Event 26 - a review of the script indicates this test was actually run on Tuesday as a by-product of other events. E-Mails being sent to COACT by sites for event verification.

Event 27 - this test was also run on Tuesday as a by-product of other events. E-Mails being sent to COACT by sites for event verification.

Event 28 - (1240) verified.

Event 29 - (1243) verified.

Event 31 - (1301) verified.

Event 30 - (1355) verified.

Event 32 - (1340) verified.

Events 33 and 34 - SATAN will not run from COACT site to participants because of the DNS registration. LIWA agrees to run a modified version (MITRE created) from one of their on-site systems to the test system to verify the claim. All icons from SATAN scripts respond except the combined icon acknowledging this is a SATAN type attack. Reason determined to be the fact that MITRE modified it sufficiently that the SATAN signature, resident in the NSX could not recognize it as SATAN.

AFWIC also running SATAN at their site. All function as claimed **(event 33 and 34) and verification accomplished.**

Note:
AFWIC running SATAN at extremely hi-speed, not encountered when input is limited by internet. Nonetheless, all attacks logged and eventually reported out as I/O allows.

Event 35 - (1435) verified by FIWC. BCBL failed due to faulty host and limited connectivity thruput.

Event 36 - (1445) verified by FIWC. BCBL again failed due to host memory and limited connectivity thruput.

Event 37-(1508) verified.

Event 38 - (1530) verified.

Event 39 - (1530) verified

Event 42 - (1540) verified

Event 43 - (1540) verified

Event 38 - (1545) rerun and again verified.

Event 39 - (1550) rerun and again verified.

Event 42 - (1550) rerun and again verified

Event 43 - (1550) verified

End of session for Thursday, 20 March 97..

Beginning of events for Friday, 21 March 97.

Review of residual problems from Thursday:

The Relational Database population feature needs to be verified. The software functions and appropriate commands need to be furnished by WheelGroup to AFWIC. Thursday, AFWIC was given a Point of Contact at WheelGroup to resolve the operation required to verify the claim. AFWIC has opened the database at their site and found it populated with the information resulting from the testing. Claim has been verified.

The Dual Homing claim could not be verified by NSA because no physical telephone lines could be obtained for use by the NSA/V2 lab (because of the unclassified nature of the test and the sensitivity of

NSA's connection of their phones to outside sources.) The test team has worked to come up with an alternate scenario. A router is being used to sub-divide a physical connection into two logical connections. SOLARIS recognizes two logical lines as dual assignment of an IP to two different locations (i.e. error). Each connection is removed from the router until the new logical line is assigned satisfactorily. Then the other lines are re-added. The claim can now be verified using the two logical lines to demonstrate dual-homing capabilities.

Event 15 - (0935) verified.

Event 16 - (0935) verified.

Event 40 - (1015) verified.

Event 41 - (1015) verified.

A review of the three day's events indicates ALL claims verified by executing all events as of 1100.

Each site is contacted and reminded to complete one Master Observation form, listing all participants, verifying equipment and software complements. This will be attached on individual forms, one for each event the site participates in, and the form completed with satisfactorily verified statement as a minimum. Other comments if desired. Complete packages to be mailed to COACT for inclusion in the report.

NSA/V2 observation forms (done by CPT Artiaga at COACT) collected and placed in master documentation envelope for inclusion in report.

ATTENDEES:

Jay Artiaga NSA/V2
Terry Losonsky, SPOCK- PM
Larry Phillips, BTG
Larry B. McGinness, COACT
Jerry Latham, WheelGroup
Mathew McDonald, CNSG/NGP
Paul Kominos, AGIC(I)